JOURNAL OF NUMBER THEORY 26, 31–37 (1987)

On the Period Length of the Generalized Lagrange Algorithm

JOHANNES BUCHMANN*

Mathematisches Institut, Universität Düsseldorf, 4000 Düsseldorf, West Germany

Communicated by H. Zassenhaus

Received November 10, 1985

The generalized Lagrange algorithm is a number geometric generalization of Lagrange's continued fraction method for computing fundamental unit and class number of real quadratic number fields. This algorithm yields a system of fundamental units and the class number of an arbitrary algebraic number field by means of computing cycles of reduced ideals. In this paper we prove that the cardinality of a cycle of reduced ideals in an ideal class of an order of an algebraic number field is $O(R)$, where R is the regulator of this order, and where the O-constant only depends on the degree of the field. We also give a lower bound on this cardinality. © 1987 Academic Press, Inc.

1. INTRODUCTION

Let K be an algebraic number field of degree $n = s + 2t$, where s is the number of real and t is the number of complex isomorphisms of K into C. These isomorphisms are denoted by $\sigma_1, \ldots, \sigma_s, \sigma_{s+1}, \overline{\sigma_{s+1}}, \ldots, \sigma_{s+t}, \overline{\sigma_{s+t}}$, and for a number $\xi \in K$ we write $|\xi|_i = |\sigma_i(\xi)|^{e_i}$ for $1 \leqslant i \leqslant s+t$, where $e_i = 1$ if σ_i is real and $e_i = 2$ if σ_i is complex.

In [2] we developed an algorithm for computing a system of fundamental units and the class number of an arbitrary order of K which is based on the following concept of neighboring minima. Let A be a free $\mathbb{Z}$-module of rank n in K. A number $0 \neq \mu \in A$ is called a *minimum* of A if there is no $0 \neq \alpha \in A$ with $|\alpha|_i < |\mu|_i$ for $1 \leqslant i \leqslant s+t$. A minimum μ' is called neighbor of μ if there is no $0 \neq \alpha \in A$ with $|\alpha|_i < \max\{|\mu|_i, |\mu'|_i\}$ for $1 \leqslant i \leqslant s+t$ and if $|\mu| \geqslant |\mu'|$.

A cycle C of minima in A was defined by the property that no two distinct elements in C are associated and that all neighbors of all elements of C are associated to elements of C. The units responsible for these

* This paper was written when the author was a Feodor–Lynen-Fellow of the Alexander von Humboldt–Stiftung and a visitor of the Department of Mathematics of the Ohio State University.

0022-314X/87 $3.00

641/26/1-3

associations are collected in the corresponding unit set $U(C)$. Such cycles as well as their corresponding unit sets turned out to be finite. Moreover such cycles are maximal systems of non associate minima in A, and all cycles are of the same cardinality. We could prove that $U(C)$ generates the unit group of the ring of multipliers $\mathcal{O}$ of A. From $U(C)$ one can compute a system of fundamental units.

Corresponding to these cycles of minima we defined *cycles of reduced ideals* in the following way. For an integral ideal B of $\mathcal{O}$ of K we denote by $L(B)$ the least positive integer contained in B, and we call B *reduced* if B is primitive and if $L(B)$ is a minimum in B. It turned out that all the reduced ideals in the class of an ideal A can be computed in the following way: Compute a cycle C of minima in A, and for each $\alpha \in C$ compute

$$B_\alpha = \frac{a}{\alpha} A$$

where a is the least common denominator of the module $(1/\alpha)A$. Then the cycle of reduced ideals $\{B_\alpha \mid \alpha \in C\}$ is the set of all reduced ideals in the ideal class of A. The class number of $\mathcal{O}$ turns out to be the number of cycles of reduced ideals in $\mathcal{O}$.

Of course the practical efficiency of this method depends on the cardinality p of the cycles of minima.

We prove in this paper, that $p = O(R)$, where R is the regulator of $\mathcal{O}$ and where the O-constants only depends on s and t. This result includes our previous result for fields unit rank 1 [1]. Moreover, it enables us for the first time to give an estimate on the period length of the (generalized) Voronoi algorithm for algebraic number fields of unit rank 2, cf. [3, 4], and of the algorithm of Steiner [6]. We also give a lower bound on p and an upper bound on the number of neighbors of a given minimum.

2. The Main Theorems

Let A be a free $\mathbb{Z}$-module of rank n in K and let p be the period length of A, i.e., the cadinality of every cycle C of minima in A. Moreover, let R be the regulator of the ring of multipliers $\mathcal{O}$ of A let w be the number of roots of unity in $\mathcal{O}$.

THEOREM 2.1. *$p \leqslant \kappa_0 R$ with*

$$\kappa_0 = \kappa_1/(\kappa_2 w)$$

$$\kappa_1 = \begin{cases} 2 \cdot 4^{n-1} & \text{for } t = 0, \\ 6 \cdot 4^s \cdot 16^{t-1} & \text{for } t \neq 0, \end{cases}$$

and

$$\kappa_2 = \begin{cases} (\log 2)^{n-1} & \text{for } t = 0 \\ 2^{t-1}(\log 2)^s(\log(2\cos(\pi/5))^{(t-1)} & \text{for } t \neq 0. \end{cases}$$

COROLLARY 2.2. *The number of reduced ideals in the maximal order of K is*

$$O(D^{1/2}\log^{n-1} D)$$

where the O-constant only depends on s and t.

COROLLARY 2.3. *The number of minima which has to be computed in the (generalized) Voronoi algorithm in order to compute the fundamental units of an order of unit rank 2 is at most $\kappa_0 \cdot R$.*

The period length in the algorithm of Steiner [6] *is at most $\kappa_0 \cdot R$.*

THEOREM 2.4. *The number of neighbors of a minimum of A is $O((\log D)^{s+t-1})$, where the O-constant only depends on s and t.*

Theorem 2.5. *$p \geqslant R/\kappa_3$ with $\kappa_3 = (\log D)^{s+t-1}$.*

3. THE PROOFS

We fix

$$r := s + t - 1,$$

$$l: K \to \mathbb{R}^r$$

$$\xi \to l(\xi) = (\log|\xi|_1, \ldots, \log|\xi|_r)^T.$$

Note that the image $l(U)$ of the unit group U of the ring of multipliers $\mathcal{O}$ of A is a r-dimensional lattice of determinant R. We fix a fundamental parallelotop F in this lattice.

LEMMA 3.1. *Let A' be a free $\mathbb{Z}$-module in K and let 1 be a minimum in A'. Moreover, let N be the number of minima μ' in A which satisfy the following conditions*

$$|\mu|_i \leqslant \lambda_i \qquad \text{for} \quad 1 \leqslant i \leqslant s + t \tag{1}$$

with

$$\lambda_i = \begin{cases} 2 & \text{for} \quad 1 \leqslant i \leqslant \min\{s, n-1\}, \\ [2\cos(\pi/5)]^2 & \text{for} \quad s < i \leqslant r, \\ 1 & \text{for} \quad i = s+t. \end{cases}$$

Then $N \leqslant \kappa_1$ *with* κ_1 *from Theorem* 2.1.

Proof. Our proof is based on the following observations:

— If more than two different number $\neq 0$ are in the real interval $[-1, 1]$, then two of them have a distance less than 1.

— If more than 4 different numbers $\neq 0$ are in the real interval $[-2, 2]$, then at least two of them have a distance less than 1.

— If more than 6 different complex numbers $\neq 0$ are in the complex unit circle, then at least two of them have a distance less than 1.

— If more than 16 different complex numbers $\neq 0$ are in the complex circle centered in 0 with radius $2\cos(\pi/5)$, then at least two of them have a distance less than 1.

Thus, if N exceeds κ_1 then there are at least two minima μ', μ'' in A' with

$$|\mu' - \mu''|_i < 1 \qquad \text{for} \quad 1 \leqslant i \leqslant s+t$$

in contradiction to the fact that 1 is a minimum in A'.

LEMMA 3.2. *For* $\mathbf{z} \in \mathbb{R}^r$ *let*

$$Q(\mathbf{z}) = \{\mathbf{z}' \in \mathbb{R}^r \mid 0 \leqslant z_i' - z_i \leqslant \log \lambda_i \text{ for } 1 \leqslant i \leqslant r\}.$$

Moreover let N *be the number of minima* μ *in* A *with* $l(\mu) \in Q(\mathbf{z})$. *Then*

$$N \leqslant \kappa_1.$$

Proof. First of all, note that $N < \infty$. In fact, we know for $\mu \in A$ with $l(\mu) \in Q(\mathbf{z})$

$$\exp z_i \leqslant |\mu|_i \leqslant \lambda_i \exp z_i \qquad \text{for} \quad 1 \leqslant i \leqslant r.$$

But if μ is a minimum, then

$$|N(\mu)| = \prod_{i=1}^{s+t} |\mu|_i \leqslant N(A)\, D^{1/2}$$

cf. [2, Proposition 2.2], where D is the absolute value of the discriminant of $\mathcal{O}$, $N(\mu)$ is the norm of μ and $N(A)$ is the norm *of* A. It follows that

$$|\mu|_{s+t} \leqslant N(A)\, D^{1/2} \Big/ \prod_{i=1}^{r} \exp z_i$$

and thus all the conjugates of all the possible μ's are bounded.

Now we choose from all minima μ in A with $l(\mu) \in Q(\mathbf{z})$ one with maximal $|\mu|_{s+t}$. Then we have for all other minima μ' in A with $l(\mu') \in Q(\mathbf{z})$

$$l_i(\mu') - l_i(\mu) \leqslant \log \lambda_i \qquad \text{for} \quad 1 \leqslant i \leqslant r,$$

and thus

$$|\mu'/\mu|_i \leqslant \lambda_i \qquad \text{for} \quad 1 \leqslant i \leqslant s+t.$$

Now we consider the module $A' = (1/\mu)\, A$. Since μ is a minimum of A we know that 1 is a minimum in A'. Moreover, for every minimum μ' in A with $l(\mu') \in Q(\mathbf{z})$ the corresponding minimum $\beta' = \mu'/\mu$ in A' satisfies (1). Thus, our lemma follows from Lemma 3.1.

LEMMA 3.3. *Let* $j \in \mathbb{Z}^+$ *and*

$$Q_j = \{\mathbf{z} \in \mathbb{R}^r \mid 0 \leqslant z_i \leqslant j \log \lambda_i, \text{ for } 1 \leqslant i \leqslant r\}.$$

Moreover, let $f(j)$ *be the number of fundamental parallelotops congruent to* F *contained in* Q_j. *Then*

$$\lim_{j \to \infty} \frac{j^r}{f(j)} = \frac{R}{\kappa_2}$$

with κ_2 *from Theorem* 2.1.

Proof. Since $j^r \kappa_2$ is the volume of Q_j and since $f(j) \cdot R$ is the volume of all the fundamental parallelotops contained in Q_j it follows that

$$\lim_{j \to \infty} \frac{j^r \kappa_2}{f(j)\, R} = 1.$$

Now we can prove Theorem 7.1.

$p \cdot w$ is bounded by the number of minima μ in A with $l(\mu) \in F$. Thus, it follows from Lemma 3.2 that for all $j \in \mathbb{Z}^+$.

$$p \cdot w \leqslant \frac{j^r \kappa_1}{f(j)}.$$

so that we finally get our result from Lemma 3.3.

Corollary 2.2 follows from Siegel's theorem [5]. Corollary 2.3 is obviously true.

We also can prove Theorem 2.4. Without loss of generality we assume that 1 is a minimum of A and we estimate the number of neighbors of 1. By Minkowski's convex body theorem we have for every neighbor η of 1 in A

$$|\eta|_i \leqslant N(A)\, D^{1/2} \qquad \text{for} \quad 1 \leqslant i \leqslant s+t,$$

and since the absolute value of the norm of η is a least $N(A)$ it follows that

$$|\eta|_i \geqslant 1/(N(A)^{r-1}\, D^{r/2}) \qquad \text{for} \quad 1 \leqslant i \leqslant s+t.$$

Since 1 is a minimum of A it follows that $N(A) \leqslant 1$, and thus we have

$$-(r/2) \cdot \log D \leqslant l_i(\eta) \leqslant (\tfrac{1}{2}) \log D,$$

and the assertion of Theorem 2.4 follows from Lemma 3.2.

For the proof of Theorem 2.5 we need

LEMMA 3.4. *Let $\mathbf{z} \in \mathbb{R}^r$. Then there is a minimum μ in A with*

$$0 \leqslant z_i - l_i(\mu) < \log D \qquad \textit{for} \quad 1 \leqslant i \leqslant r.$$

Proof. Put $y_i = \exp z_i$ for $1 \leqslant i \leqslant r$ and $y_{s+t} = 1/\prod_{i=1}^{r} y_i$. By Minkowski's convex body theorem, there is a minimum μ in A with

$$|\mu|_i \leqslant y_i \qquad \text{for} \quad 1 \leqslant i \leqslant r$$

and

$$|\mu|_{s+t} \leqslant y_{s+t} N(A)\, D^{1/2}.$$

Since $|N(\mu)| \geqslant N(A)$, it follows that

$$|\mu|_i \geqslant y_i / D^{1/2} \qquad \text{for} \quad 1 \leqslant i \leqslant r,$$

and this proves the assertion.

LEMMA 3.5. *Let $j \in \mathbb{Z}^+$ and let*

$$Q_j = \{\mathbf{z} \in \mathbb{R}^r \mid 0 \leqslant z_i \leqslant j \log D\}.$$

Moreover, let $f(j)$ be the number of fundamental parallelotops congruent to F which have a non-empty intersection with Q_j. Then

$$\lim_{j \to \infty} \frac{j^r}{f(j)} = \frac{R}{\kappa_3}.$$

Proof. Since $j^r\kappa_3$ is the volume of Q_j and since $f(j)\cdot R$ is the volume of the union of the covering fundamental parallelotops, we have

$$\lim_{j\to\infty}\frac{j^r\kappa_3}{f(j)\,R}=1.$$

Now we prove Theorem 2.5.

By Lemma 3.4 we find that there are at least j^r distinct minima μ in A with $l(\mu)\in Q_j$ and with the property that no two of these minima are associated by roots of unity. Hence we have for all $j\in\mathbb{Z}^+$,

$$p\geqslant j^r/f(j)$$

so that we get finally our result from Lemma 3.5.

REFERENCES

1. J. BUCHMANN, Abschätzung der Periodenlänge einer verallgemeinerten Kettenbruchentwicklung, *J. Reine Angew. Math.* **361** (1985), 27–34.
2. J. BUCHMANN, On the computation of units and class numbers by a generalization of Lagrange's algorithm, *J. Number Theory* **26** (1987), 8–30.
3. J. BUCHMANN, A generalization of Voronoi's unit algorithm I, II. *J. Number Theory* **20** (1985), 177–209.
4. B. N. DELONE AND B. K. FADEEV, The theory of irrationalities of the third degree Amer. Math. Soc. Transl. Amer Math. Soc., Providence, R.I., 1964.
5. C. L. SIEGEL, Abschätzung von Einheiten, Ges. Abh. IV, pp. 66–81.
6. R. P. STEINER, On the units in algebraic number fields, *in* "Proceedings, 6th Manitoba Conf., Numer. Math., 1976, pp. 413–435.